IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA,	§	
	§	
Plaintiff,	§	
	§	
VS.	§	Criminal No. 3:16-CR-305-D(1)
	§	
PAUL TERRY PERDUE,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION AND ORDER

The instant motions to suppress and dismiss the indictment challenge the Federal Bureau of Investigation's ("FBI's") seizure of a computer server that hosted a child pornography website called "Playpen," and the FBI's ensuing operation of the website on a government server. Following a hearing, and for the reasons that follow, the court denies defendant Paul Terry Perdue ("Perdue's") motions.[1]

I

The facts of this case that are material to the court's decision are undisputed. In early 2015, acting on a tip from a foreign law enforcement agency, the FBI located and seized a computer server that contained a child pornography website called Playpen. Playpen existed as a hidden website on the Tor Network,[2] also known as the dark web. Through

[1] Pursuant to Fed. R. Crim. P. 12(d), the court sets forth its essential findings in this memorandum opinion and order.

[2] "Tor" refers to The Onion Router, which was originally developed by an entity of the United States Government.

sophisticated encryption, the Tor Network anonymizes and actively conceals identifying information about website users, including a user's true Internet Protocol ("IP") address. To access Playpen, it was necessary for users to know the website's address on the Tor Network. Users could not, for example, stumble upon Playpen while browsing the Internet. Once on the Playpen website, users logged in with dedicated usernames and passwords. Playpen offered users various forums for different child pornography topics, including "Incest" and "Toddlers." Inside each forum were discussion posts, images, and videos related to the particular topic.

Because the Tor Network anonymizes its users, the FBI could not uncover who was operating or accessing the Playpen website through normal investigative techniques. The FBI devised a plan to investigate Playpen's users, who would normally be untraceable. The plan called for the FBI to copy the Playpen server and continue to operate the Playpen website on the FBI server. While operating the website, the FBI would use a network investigative technique ("NIT") that allowed it to retrieve information from the computers of the persons who logged in to the Playpen website. The NIT—computer code developed by the FBI—would be attached to various files uploaded to Playpen. When the website user downloaded a file, the NIT would force the user's computer to send to the FBI the user's actual IP address and other identifying information. With the actual IP address, the FBI could identify and locate the user.

Acting according to the plan, the FBI copied the Playpen server and brought it to a government facility located in the Eastern District of Virginia. On February 20, 2015 the FBI applied for and obtained from a United States Magistrate Judge of the Eastern District of Virginia a search warrant (the "NIT Warrant") authorizing the FBI to deploy the NIT program for a period of up to 30 days.

On or about February 23, 2015, Perdue accessed the Internet from his residence using a personal computer. Using the Tor Network, he logged in to the Playpen website and clicked on a post entitled, "8 Year Old Blonde," which contained child pornography. As the content from this post downloaded onto the computer, the NIT computer code was sent automatically. The NIT relayed Perdue's IP address and other information back to the FBI in the Eastern District of Virginia.

Based on this information, the FBI issued a subpoena to AT&T, the Internet service provider connected with Perdue's IP address, and learned that Perdue was the account holder associated with the address. The FBI obtained a warrant to search Perdue's residence, and it found (1) a computer containing child pornography, and (2) a flash drive containing an 80-page Microsoft Word document containing links to child pornography websites. Perdue subsequently confessed to accessing Playpen and using the Tor Network to obtain child pornography.

The grand jury later indicted Perdue for the offenses of receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), and possession of child pornography involving a prepubescent minor, in violation of 18 U.S.C. § 2252A(a)(5)(B). Perdue moves to suppress all evidence obtained from the NIT, alleging that the authorizing warrant was made without jurisdiction under 28 U.S.C. § 636(a) and Fed. R. Crim. P. 41. He also moves to dismiss the indictment. The government opposes both motions.

II

The court first considers Perdue's motion to suppress evidence that he alleges was collected in violation of the Fourth Amendment.[3]

A

The general rule under the Fourth Amendment is that searches of private property are reasonable if conducted pursuant to a valid warrant issued upon probable cause. *See, e.g.*, *Katz v. United States*, 389 U.S. 347, 357 (1967). "A defendant normally bears the burden of proving by a preponderance of the evidence that the challenged search or seizure was unconstitutional." *United States v. Waldrop*, 404 F.3d 365, 368 (5th Cir. 2005) (citing *United States v. Guerrero-Barajas*, 240 F.3d 428, 432 (5th Cir. 2001)). "The exclusionary rule prohibits introduction at trial of evidence obtained as the result of an illegal search or seizure." *United States v. Runyan*, 275 F.3d 449, 466 (5th Cir. 2001). The exclusionary rule also "encompass[es] evidence that is the indirect product or 'fruit' of unlawful police conduct." *Id.* (citing *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)).

[3] The court assumes *arguendo* that the NIT constituted a search that triggered the protections of the Fourth Amendment.

B

1

Perdue contends that the magistrate judge in the Eastern District of Virginia who issued the NIT Warrant lacked authority under both Fed. R. Crim. P. 41(b) (2015)[4] and § 636(a) of the Federal Magistrate Judges Act, 28 U.S.C. § 636(a),[5] to authorize the search of a computer in Texas. The government responds that the NIT is functionally a tracking device that "was used to track the movement of [information] both within and outside of Virginia." Gov't Br. 10. According to the government, "[t]he NIT program, by way of operation, used [a communication stream between the government's server in Virginia and Perdue's computer in Texas] to track from where Perdue's computer signal emanated." *Id.*

[4] Amended Rule 41(b)(6), which took effect on December 1, 2016, remedies the limitation on the magistrate authority that is discussed in this and several other decisions related to the NIT Warrant. It provides:

> (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
> (A) the district where the media or information is located has been concealed through technological means; or
> (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

The parties agree that this new rule is inapplicable in this case.

[5] Relevant here, § 636(a) provides that magistrate judges shall have "within the district . . . all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts."

2

Rule 41(b)(4) provides that "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." A "tracking device" is "an electronic . . . device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117; *see also* Rule 41(a)(2)(E) (incorporating definition in § 3117). And the rules indicate that "property" includes "information." Rule 41(a)(2)(A).

The courts that have considered the NIT Warrant have split on the issue. *See United States v. Torres*, 2016 WL 491223, at *4 (W.D. Tex. Sept. 9, 2016) (collecting cases). Courts that have held that Rule 41(b) was not violated have concluded that the defendants "voluntarily and deliberately came to the Eastern District of Virginia when [they] took affirmative steps to log into the Playpen website by entering a username and password." *United States v. Sullivan*, 2017 WL 201332, at *6 (N.D. Ohio Jan. 18, 2017); *see also United States v. Anzalone*, ___ F.Supp.3d ___, 2016 WL 5339723, at *9 (D. Mass. 2016) (collecting cases). It was therefore permissible for the magistrate judge to authorize affixing a tracking device—i.e., the NIT code—to the defendants' computers once they were present in the district. Courts that have held that the magistrate judge violated Rule 41(b) have reasoned that the government's defense of the magistrate judge's authority stretches the Rule. *See, e.g.*, *United States v. Hammond*, ___ F.Supp.3d ___, 2016 WL 7157762, at *4 (N.D. Cal. Dec. 8, 2016) ("[Defendant's] computer is a physical object that at all times remained in his home in the Northern District of California, and the download, too, occurred here and not 'virtually' in the Eastern District of Virginia.").

The court agrees with the courts that have concluded that Rule 41(b)(4) does not extend to the NIT Warrant. Although caselaw suggests that the court is to construe Rule 41(b) broadly, *see United States v. N.Y. Tel. Co.*, 434 U.S. 159, 169 (1977) (holding that Rule 41(b) "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause"), it cannot render it meaningless. As one court has explained:

> [i]f the "installation" occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [defendant's] computer, applying the tracking device exception again fails, because [defendant's] computer was never physically located within the Eastern District of Virginia.

United States v. Michaud, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016). Accordingly, the court holds that the NIT Warrant exceeded the magistrate judge's authority under Rule 41(b) by authorizing the search of a computer in Texas.

C

Although the NIT Warrant violated Rule 41(b), it does not follow automatically that the search and seizure in this case should be suppressed.

1

The exclusionary rule precludes the government from relying on illegally-seized evidence. *United States v. Houltin*, 566 F.2d 1027, 1030 (5th Cir. 1978). "The purpose of the exclusionary rule is to deter unlawful police conduct." *United States v. Pope*, 467 F.3d 912, 916 (5th Cir. 2006). This purpose will not be served, and thus the rule is inapplicable, where evidence is obtained in "objectively reasonable good-faith reliance upon a search warrant." *Id.* (citations and internal quotation marks omitted). "Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith." *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003) (citing *United States v. Leon*, 468 U.S. 897, 921-25 (1984)). The good-faith exception cannot apply if "the issuing magistrate/judge was misled by information in an affidavit that the affiant knew was false or would have known except for reckless disregard of the truth[.]" *Id.* at 399 (quoting *United States v. Webster*, 960 F.2d 1301, 1307 n.4 (5th Cir. 1992) (per curiam)). "The 'good faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization.'" *Pope*, 467 F.3d at 917 (quoting *Leon*, 468 U.S. at 922 n.23).

In the context of a Rule 41 violation,

> where there is no constitutional violation nor prejudice in the sense that the search would likely not have occurred or been as abrasive or intrusive had Rule 41 been followed, suppression . . . is not appropriate if the officers concerned acted in the affirmative good faith belief that the warrant was valid and authorized their conduct.

United States v. Comstock, 805 F.2d 1194, 1207 (5th Cir. 1986). This is because the balance of interests inherent in an exclusionary rule analysis "weighs much less heavily [when] the [Rule 41] violation is neither of constitutional dimensions nor intentional." *Id.* at 1210.

2

Perdue maintains that, as a threshold matter, the good-faith exception cannot apply where a warrant was void at its outset. *See United States v. Levin*, 186 F.Supp.3d 26, 38-42 (D. Mass. 2016) (holding that good-faith exception is inapplicable to NIT because NIT Warrant was void *ab initio*). The court is unaware of any binding precedent in this circuit that restricts the exception in this manner, and it therefore declines to adopt this rule.[6]

3

Perdue maintains that a Rule 41 violation is a *per se* constitutional violation because Rule 41 concerns substantive judicial authority, and a violation therefore "constitutes a jurisdictional flaw that cannot be excused as a technical defect." D. Br. 15 (quoting *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013)) (internal quotation marks omitted). The court disagrees. The Fourth Amendment does not address the powers of magistrate judges or district judges, nor does it address whether judges' power extends beyond district boundaries. The Fourth Amendment simply requires, in pertinent part, that a warrant be issued by a "neutral magistrate." U.S. Const. amend. IV. Thus any more specific restrictions regarding who can issue a particular type of warrant are statutory or rule creations that do not

[6] The Sixth Circuit once followed this rule, but later abandoned it because it was "no longer clearly consistent with current Supreme Court doctrine[.]" *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010).

implicate the Fourth Amendment. *See, e.g.*, *United States v. Deichert*, 2017 WL 398270, at *8 (E.D.N.C. Jan. 28, 2017) (holding that NIT Warrant Rule 41 violation did not implicate Fourth Amendment because "while the law requires due regard for geographic boundaries created by statute, violations based on such geographic boundaries cannot rise to the level of unconstitutionality.").

4

The court must also evaluate whether the Rule 41(b) violation prejudiced Perdue by subjecting him to a search that would not have occurred or that would have been less intrusive absent the violation. *See Comstock*, 805 F.2d at 1207. Perdue contends he suffered prejudice because he would not have been subjected to the search absent the Rule 41(b) violation. The court disagrees.

The version of Rule 41(b) in effect on February 20, 2015 would not have permitted a magistrate judge of the Eastern District of Virginia to issue the NIT Warrant. *See supra* § II(B)(2). But it would not have precluded a district judge in that district from issuing the same warrant. *United States v. Jean*, ___ F.Supp.3d ___, 2016 WL 4771096, at *12 n.16 (W.D. Ark. Sept. 13, 2016) ("District judges are not limited by Rule 41(b) as magistrate judges are. Instead, district judges may issue warrants to search property located outside their judicial districts when the requirements of the Fourth Amendment are met."). Perdue does not contend that the NIT Warrant is not supported by probable cause. Accordingly, had a district judge been presented the same warrant application, the district judge would have been authorized to issue a warrant for the search of Perdue's computer in Texas. The court therefore concludes that the Rule 41(b) violation was technical.

5

The final aspect of the court's analysis is whether law enforcement acted with an intentional disregard of Rule 41(b). Perdue contends that the good-faith exception is inapplicable because the government willfully violated Rule 41(b).

Perdue contends that the FBI agents responsible for securing the NIT Warrant were "reckless, grossly negligent," or at the very least acting pursuant to "systematic negligence" in their pursuit of a warrant the violated Rule 41. D. Br. 19 (internal quotation marks omitted). Perdue points to circumstantial evidence, including that the Justice Department was aware that similar searches had been rejected under Rule 41[7] and allegations of forum-shopping, to illustrate that the government's violations were intentional. Regardless of the agents' subjective beliefs and the existence of potentially contrary, albeit non-binding, authority, it was far from clear at the time that the NIT Warrant violated Rule 41(b). In fact, several courts have held that the NIT Warrant did *not* violate Rule 41(b). *See, e.g., Jean*, 2016 WL 4771096, at *16-17. Accordingly, although this court has held that the NIT warrant violated Rule 41(b) by exceeding the magistrate judge's authority, the court also concludes that the government did not intentionally violate the Rule. The court therefore concludes, as has nearly every other court to consider this question, that the good-faith

[7] Perdue relies on two cases, neither of which was binding authority in the Eastern District of Virginia on February 20, 2015. *Glover,* 736 F.3d at 515; *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp. 2d 756-61 (S.D. Tex. 2013).

exception applies to the execution of the NIT Warrant. *See, e.g.*, *Anzalone*, 2016 WL 5339723, at *10. The court therefore denies the motion to suppress.

III

The court now considers Perdue's motion to dismiss the indictment. Perdue contends that the government's control and maintenance of the Playpen website was so outrageous as to constitute a due process violation under the Fifth Amendment.

A

The Supreme Court has contemplated that it "may some day be presented with a situation in which the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction[.]" *United States v. Russell*, 411 U.S. 423, 431-32 (1973). The conduct that is so outrageous as to warrant dismissal is undeveloped in the caselaw. The Fifth Circuit in *United States v. Tobias*, 662 F.2d 381, 386 (5th Cir. Unit B Nov. 1981), provided a broad framework. In *Tobias* the court affirmed the denial of dismissal where the government agent, posing as a chemical supplier, convinced the defendant to manufacture Phencyclidine and agreed to send the defendant "everything he needed to get set up." *Id.* at 383-84. Although the Fifth Circuit concluded that this was a permissible infiltration of criminal activity as a means of investigation, it noted that the government cannot "instigate the criminal activity, provide the place, equipment, supplies and know-how, and run the entire operation with only meager assistance from the defendants without violating fundamental fairness." *Id.* at 386.

B

Perdue maintains that the government's operation of the Playpen website crossed this outer limit set by *Tobias*. He posits that the government instigated the activity by relaunching the Playpen website from its own server in Virginia, and thereafter expanded the scope of the operation and "facilitated the uploading and redistribution of thousands of new items of child pornography" with its maintenance of the website. D. Mot. to Dis. Br. 4. Perdue contends that the government essentially ran the entire criminal enterprise, with defendants like Perdue playing a small role.

The court disagrees with Perdue's argument, as has every other district court that has considered it. *See, e.g., United States v. Tran*, ___ F.Supp.3d ___, 2016 WL 7468005, at *3 (D. Mass. 2016) ("Every district court to consider this same argument has found it wanting."). It is undisputed that the government did not create the Playpen website. It did not alter the site's functionality, add additional child pornography, or actively solicit new users. Rather, the government simply maintained the preexisting structure that Playpen website visitors allegedly used to distribute and receive child pornography among themselves.

Moreover, Perdue cannot maintain that he provided only "meager assistance" to the government. *See Tobias*, 662 F.2d at 386. By the very nature of the Tor Network, Perdue must have actively sought out Playpen and registered for the site with a username and password. In order to activate the NIT, Perdue must have downloaded specific images of child pornography from the Playpen website. This is more than meager assistance; it is active participation.

Accordingly, because Perdue cannot show that the government violated his due process rights, the court denies his motion to dismiss.

* * *

For the reasons explained, the court denies Perdue’s motion to suppress and his motion to dismiss.

SO ORDERED.

February 17, 2017.

Sidney A. Fitzwater

SIDNEY A. FITZWATER
UNITED STATES DISTRICT JUDGE